OpenChainJapan Tooling Sub Working Group

OpenChain仕様の活用を視野に入れたSW360運用について

TOSHIBA

株式会社 東芝　研究開発本部

ソフトウェア技術センター

オープンソース技術部　浜　功樹

kouki1.hama@toshiba.co.jp

Contents

01

前回の振り返り「SW360とは？」

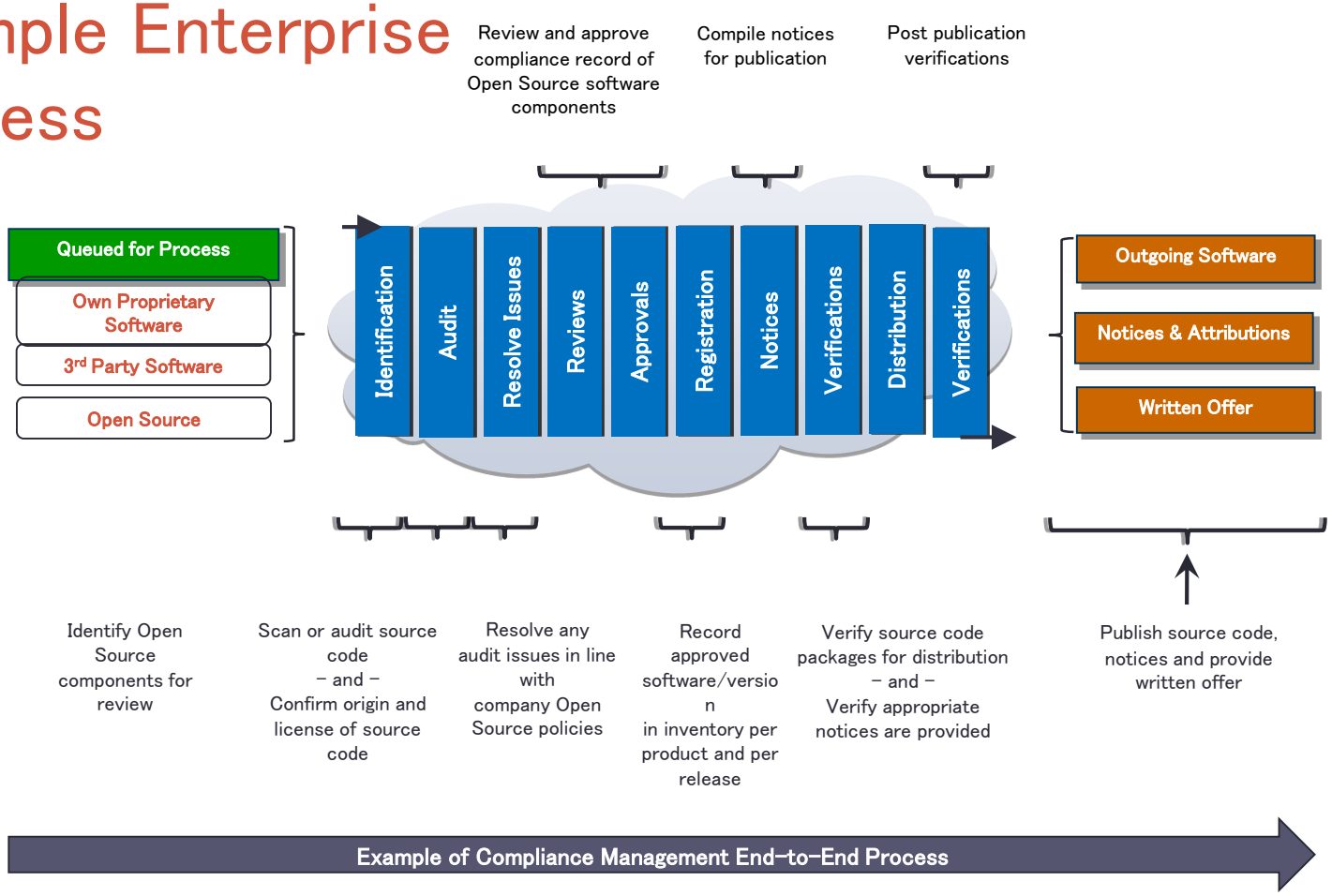
SW360とSW360のインストール方法

- 前回の発表
  - https://wiki.linuxfoundation.org/openchain/jwg_tooling_sg_page
- インストール方法紹介
  - OSS管理ツール SW360 - オープンソースをオープンソースで管理しよう
    - https://qiita.com/K-Hama/items/90a6105a16400ce3e718
- 設定方法
  - OSS管理ツール SW360 - オープンソースをオープンソースで管理しよう （２． 設定編 その1）
    - https://qiita.com/K-Hama/items/c66d9becf9aeb8f8863e
- Github
  - https://github.com/eclipse/sw360
- メーリングリスト
  - https://accounts.eclipse.org/mailing-list/sw360-dev
  - https://accounts.eclipse.org/mailing-list/sw360-users

02

SW360とOpenChainの仕様

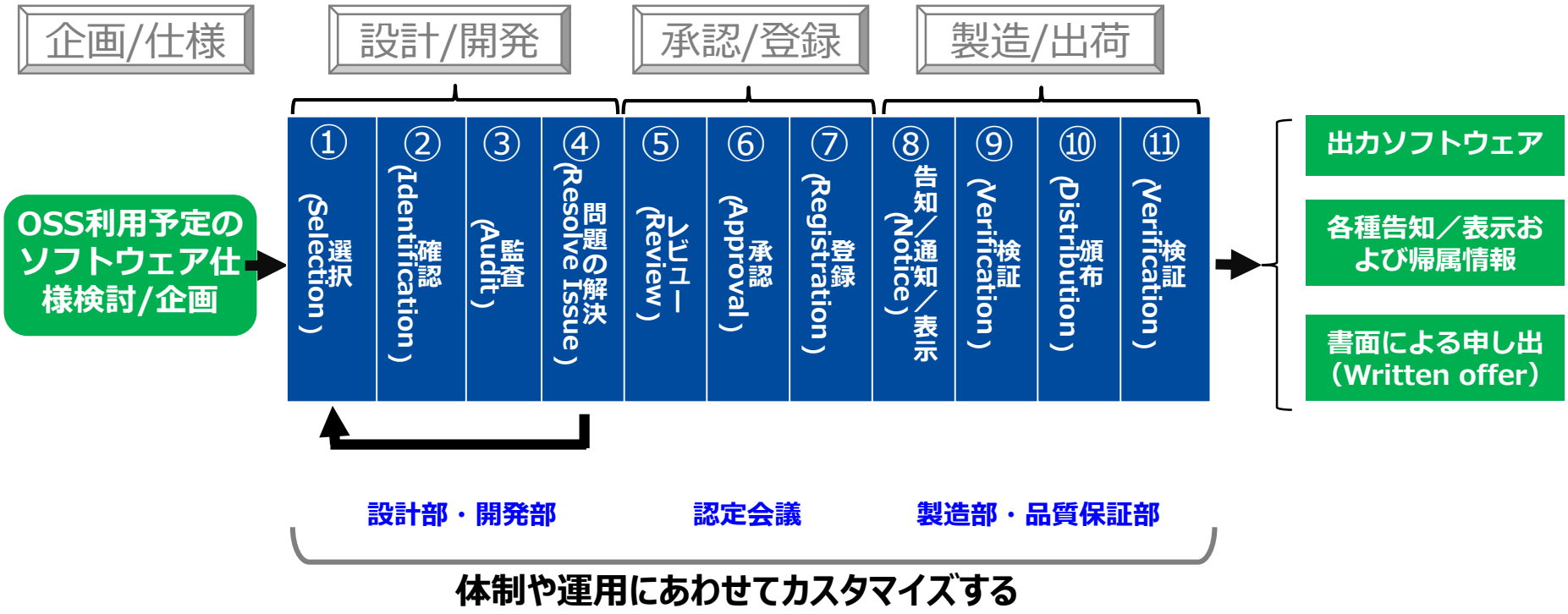
Example Enterprise Process



出典
https://www.openchainproject.org/resources

OSSを利用するためのプロセス

Open Chain プロセスに準拠



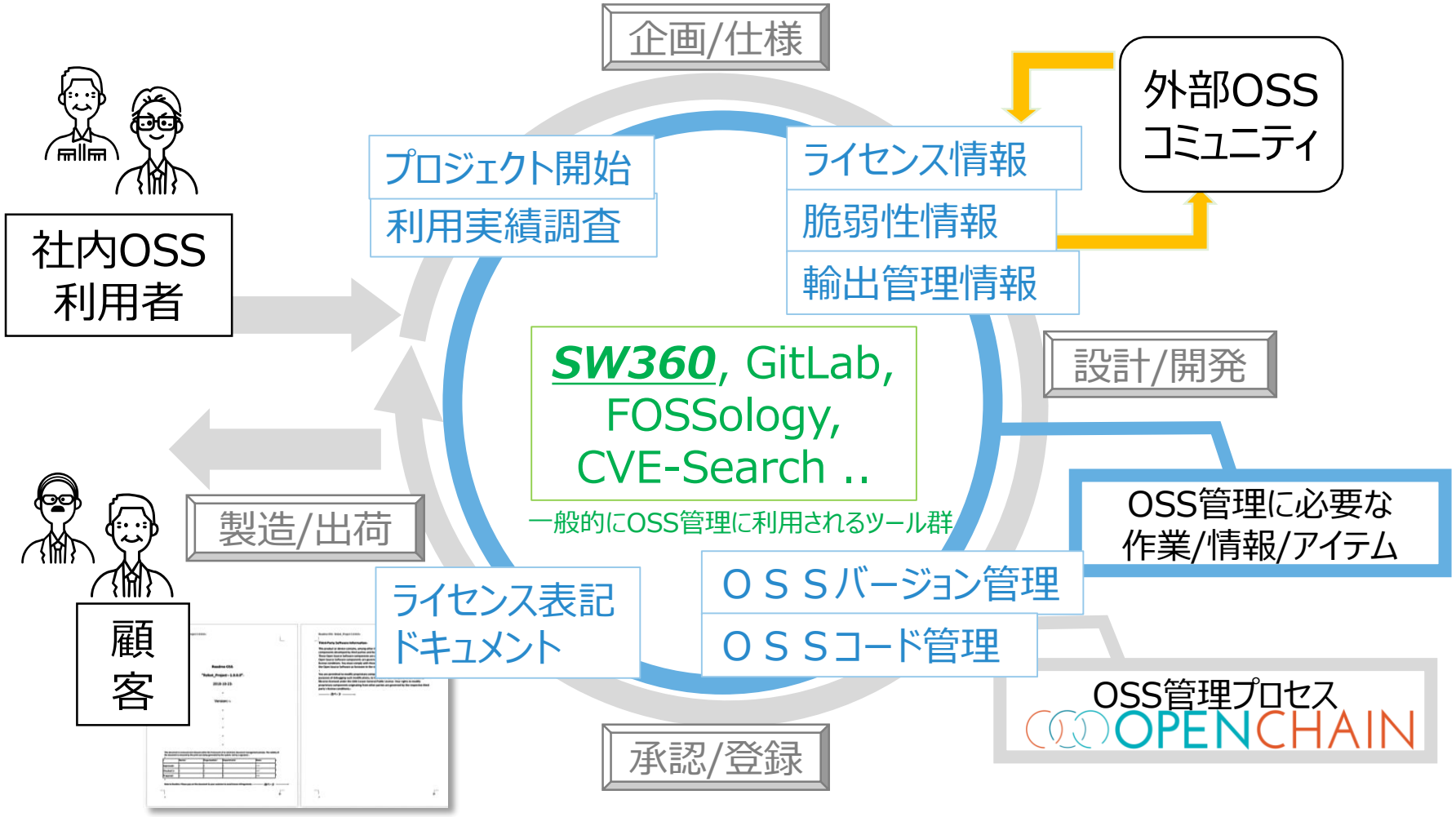
1.2準拠

参考： https://www.openchain.org
https://www.slideshare.net/ShaneCoughlan3/giving-everyone-access-to-open-source-best-practices-the-openchain-curriculum

備考：ステップ①選択を追加

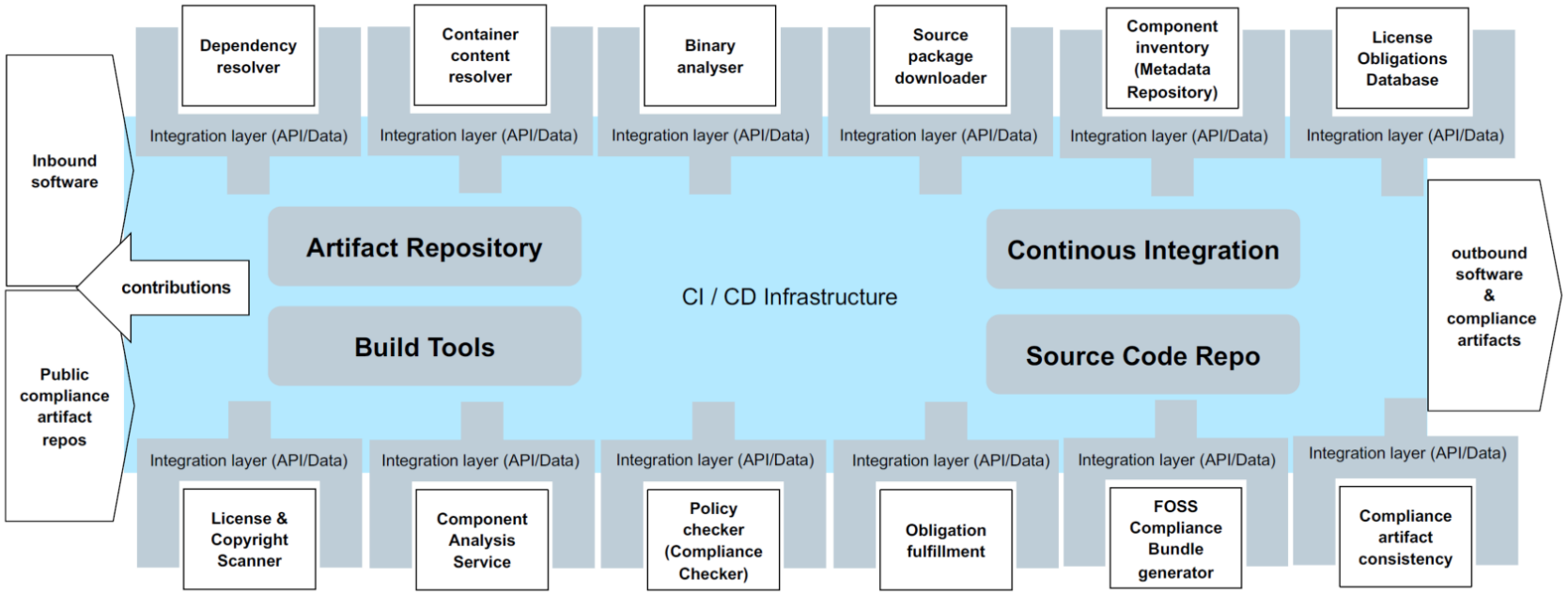
OSS管理とSW360

OSS活用・管理プロセスと一体運用（概案）



Big Picture – Integrated Compliance Toolchain

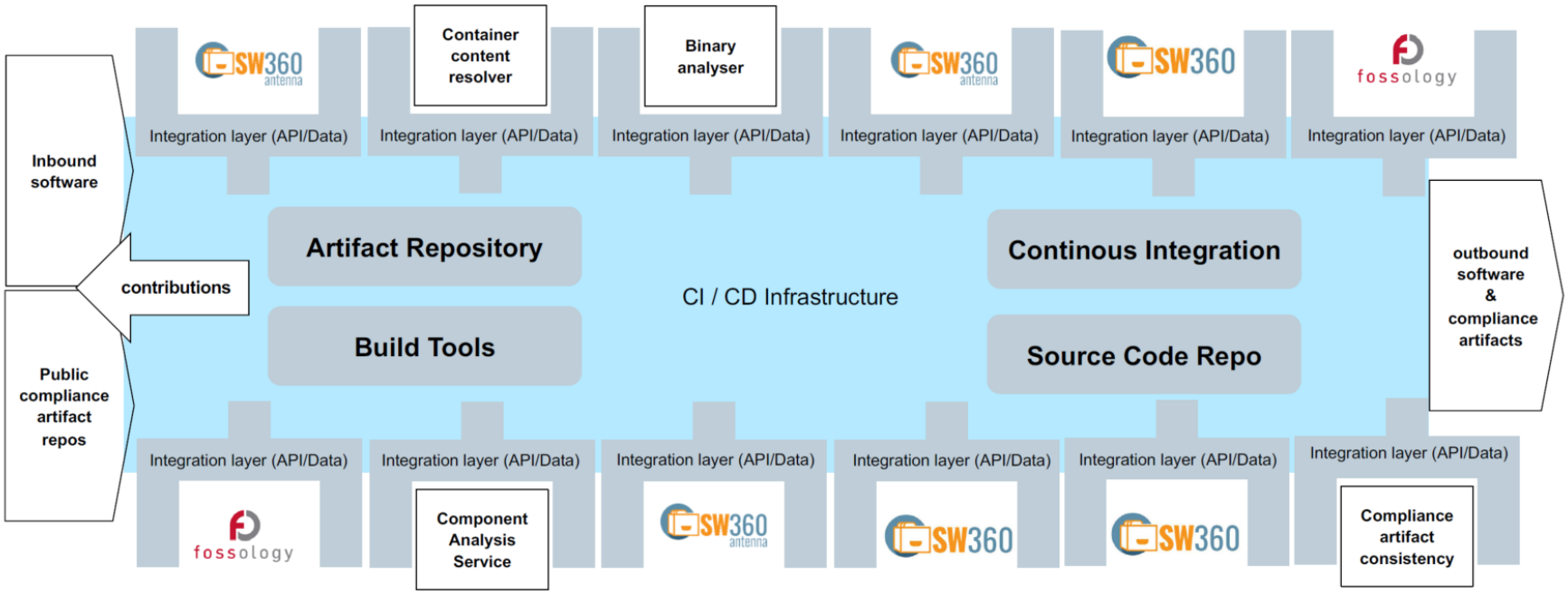
SIEMENS
Ingenuity for life



出典([Openchain-japan-wg]メーリングリスト)
https://lists.linuxfoundation.org/mailman/private/openchain-japan-wg/attachments/20190510/f0fdae60/attachment.pdf

Big Picture – Integrated Compliance Toolchain Instance

SIEMENS
Ingenuity for life



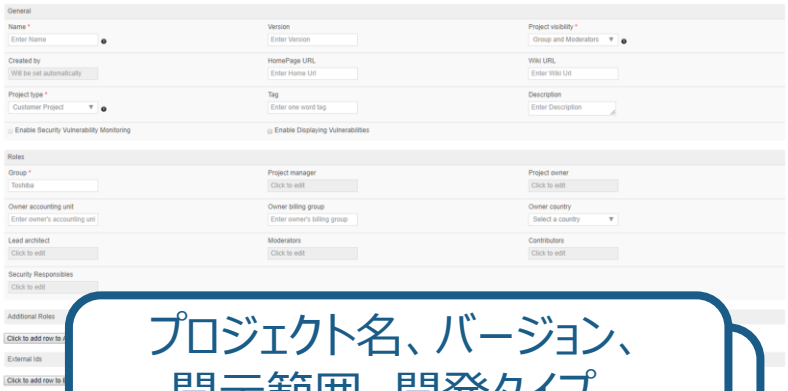
出典([Openchain-japan-wg]メーリングリスト)
https://lists.linuxfoundation.org/mailman/private/openchain-japan-wg/attachments/20190510/f0fdae60/attachment.pdf

SW360で情報管理

OSS情報のバージョン管理システム

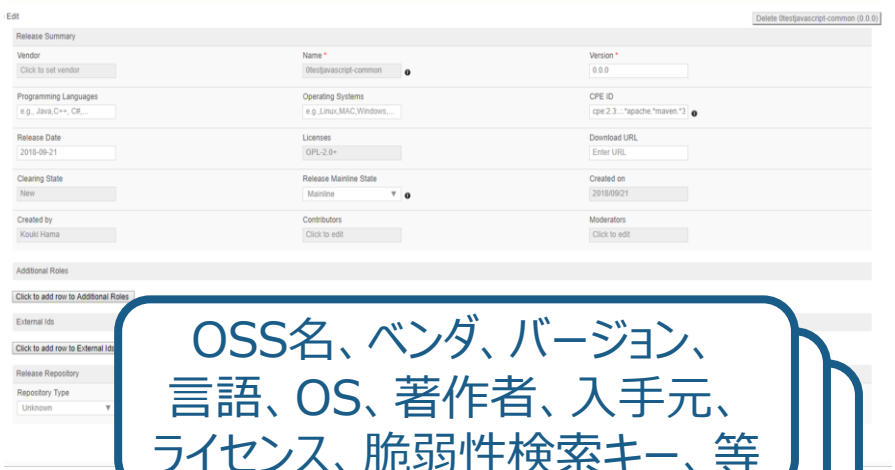
プロジェクト情報とOSSコンポーネントを紐付けて管理する

プロジェクト管理画面



プロジェクト名、バージョン、
開示範囲、開発タイプ、
開発部門、開発リーダ、等

OSSごとのコンポーネント管理画面



OSS名、ベンダ、バージョン、
言語、OS、著作者、入手元、
ライセンス、脆弱性検索キー、等

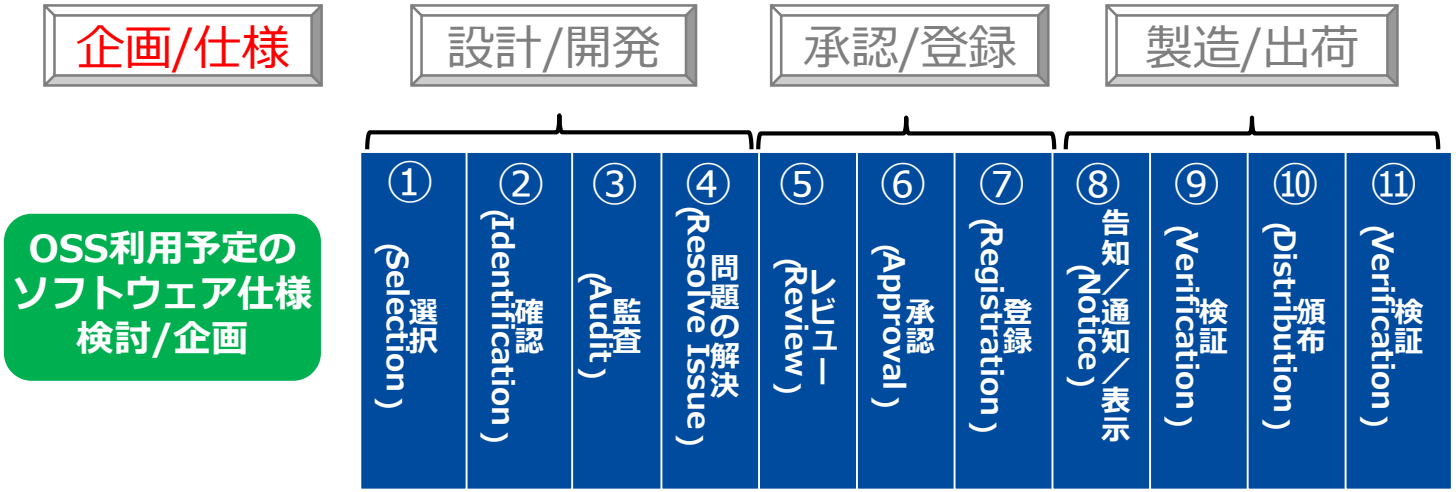
OSS情報

相互に関連付けられる

OSS利用時の導入

SW360:

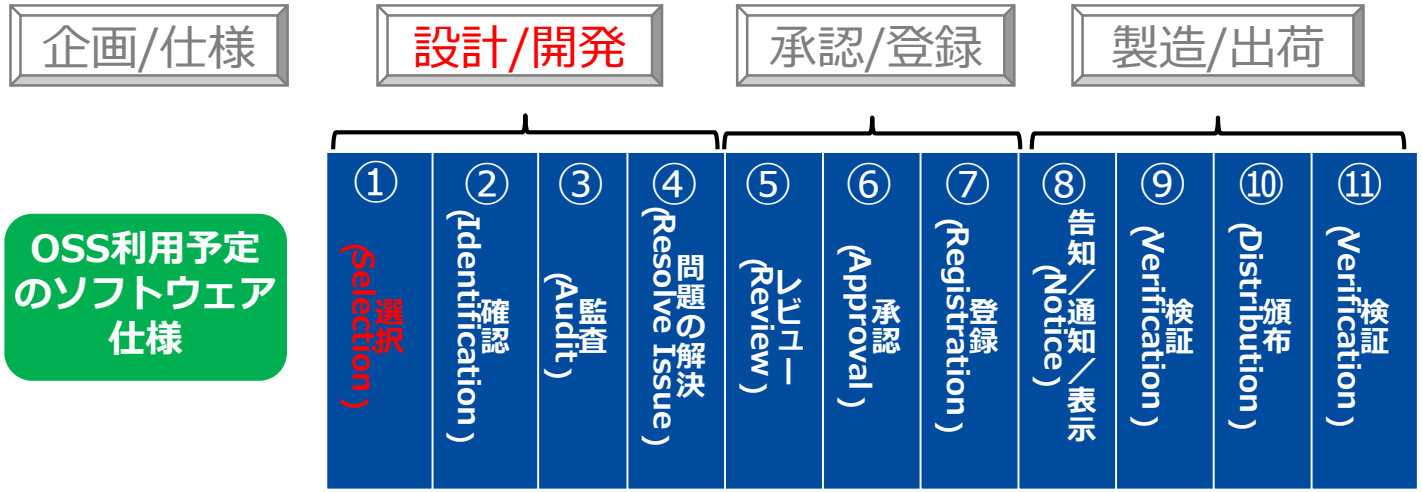
- 該当するプロジェクトを作成する
- 既存のプロジェクトがある場合は、適切であることを確認する
- プロジェクトに携わるメンバを決め、プロジェクトに対するアクセス権限を設定する



① 選択

SW360：

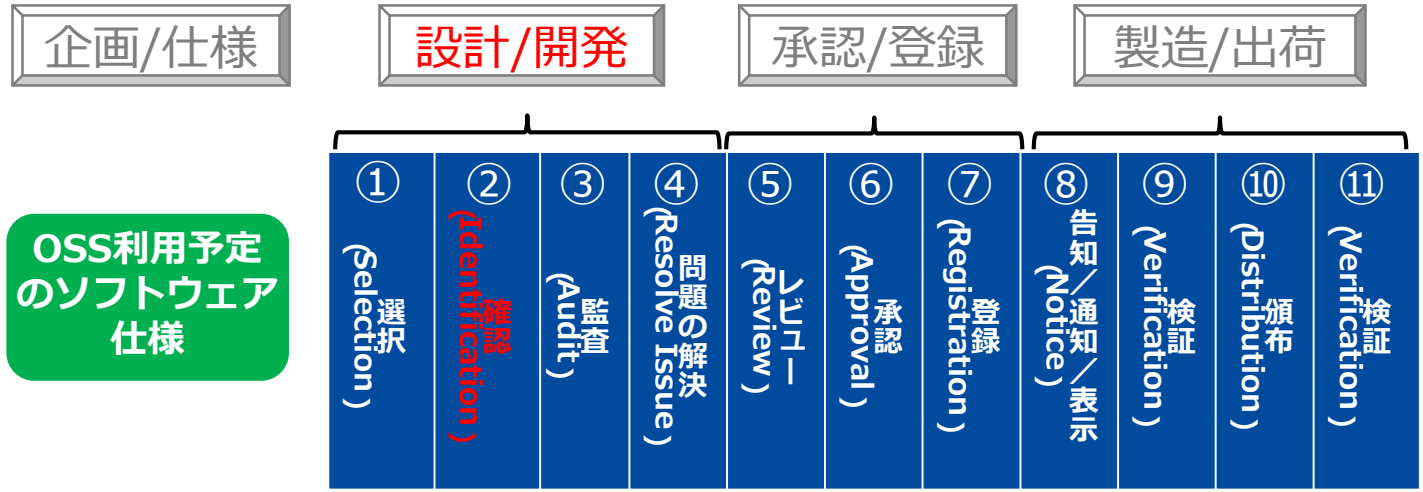
- 使用予定のコンポーネント(OSS,商用ソフト等)をリストアップ
- 必要に応じて過去の使用実績などを参照する



② 確認

SW360：

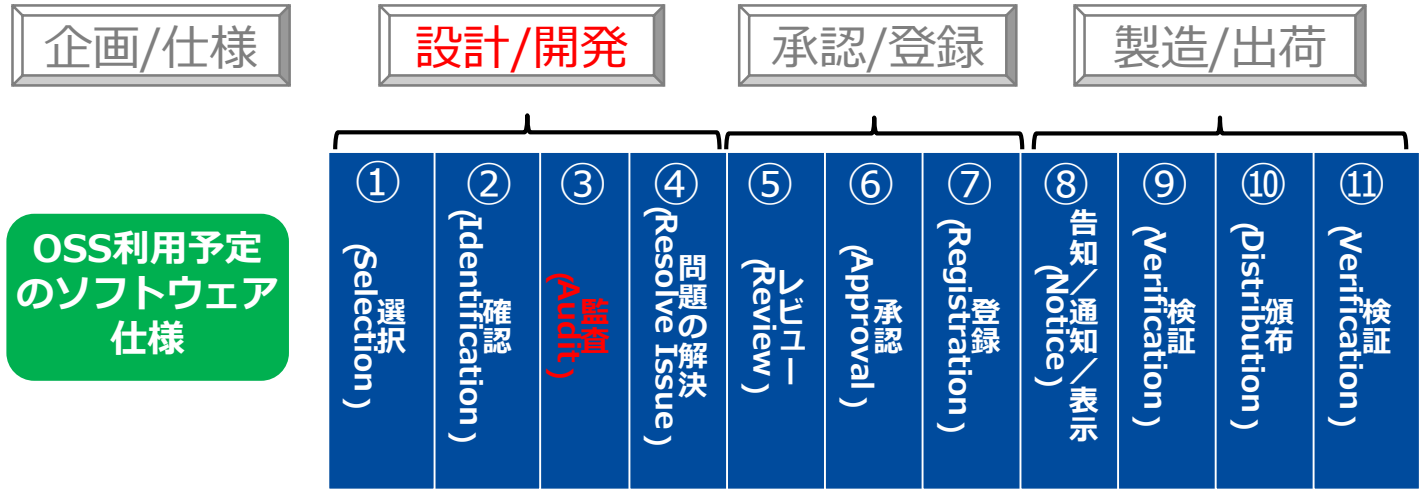
- 使用コンポーネント(OSS)情報(名称、バージョン、入手元、その他入力可能な情報)登録する
- OSS入手元のソースコードを確認する
- OSSを使用する開発に利用することを登録
- OSS管理責任者が承認



③ 監査

SW360(要検討)：

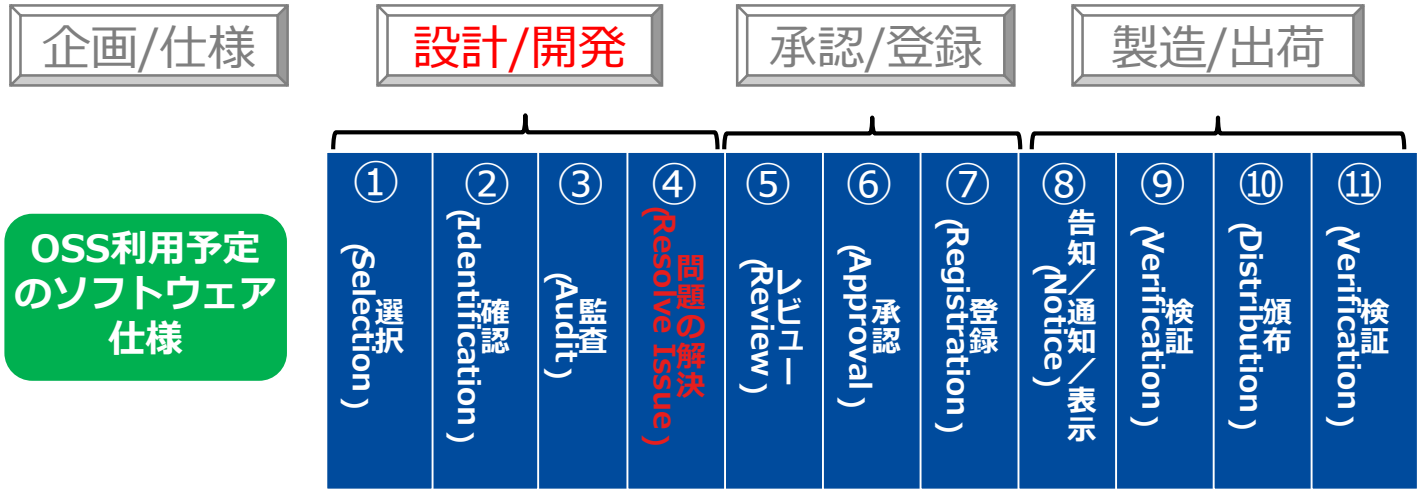
- OSSソースコードを登録（バージョン管理）
- ライセンススキャン　(ライセンス情報取得/Fossology)
- コードスキャン　(未知のOSS検出)
- OSS使用状況を登録　(設計仕様管理)
- コンポーネント脆弱性検索キー(CPE ID)を設定
- コンポーネント輸出管理関連情報を設定



④ 問題の解決

SW360：

- ロコンポーネント登録情報の更新
- ロ構成管理表 (BoM) 出力　（レビュー用情報）



⑤ レビュー

SW360(要検討)：

□レビュー実施記録

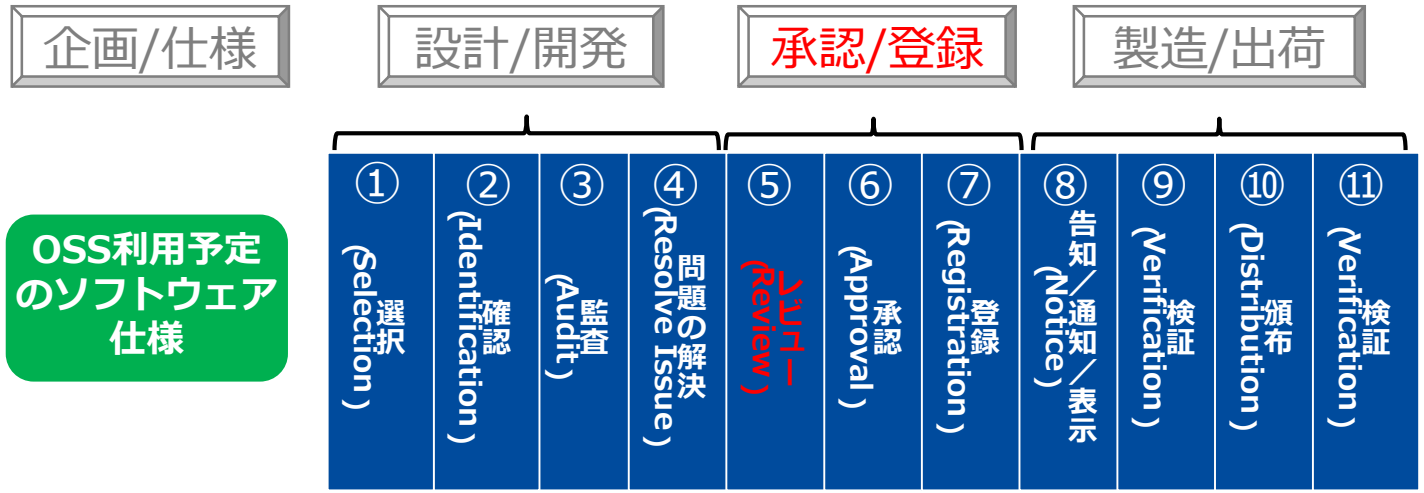
例えば以下のレビュー結果を保存

・OSSライセンスの問題の解決が完了していることを検証

・アーキテクチャ・レビュー：OSSと自製コードの構造検証

・ リンク解析レビュー：LGPLのリンク方法について検証

→　問題が見つかった場合は開発部門へ対応を依頼するような機能が必要？



⑥ 承認

SW360(要検討)：

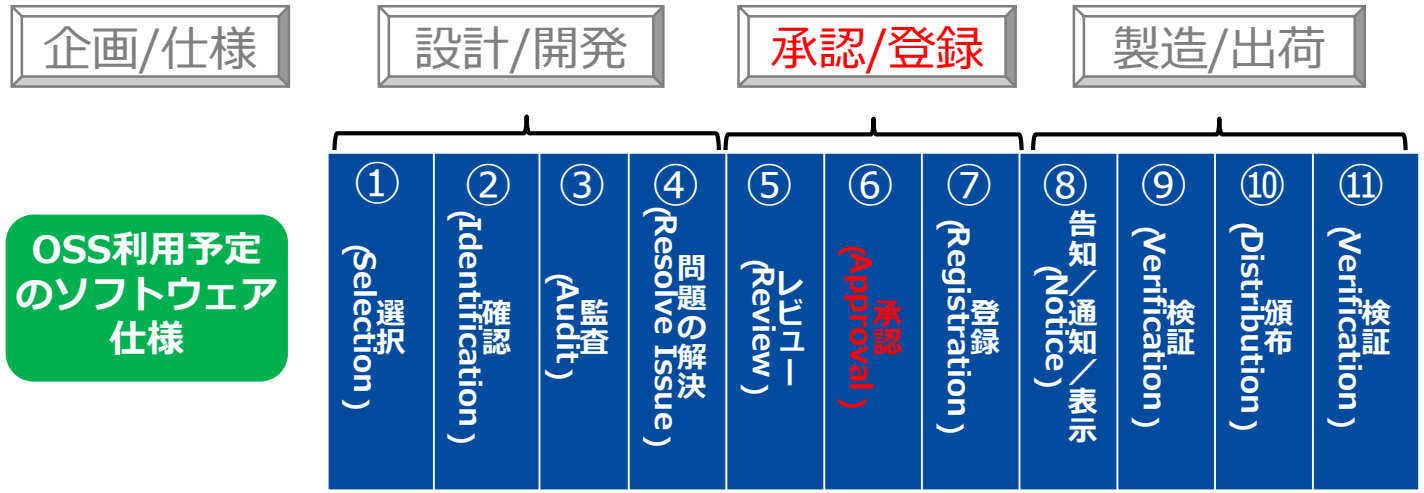
□承認（承認者、日時、付帯条件、等）を記録

ここでやりたいこと

・OSS使用に関する全ての確認、レビューが完了していることを検証する

・承認する場合は、製品部へOSS使用条件を伝達する

・否認する場合は、開発担当へ理由を明らかにする

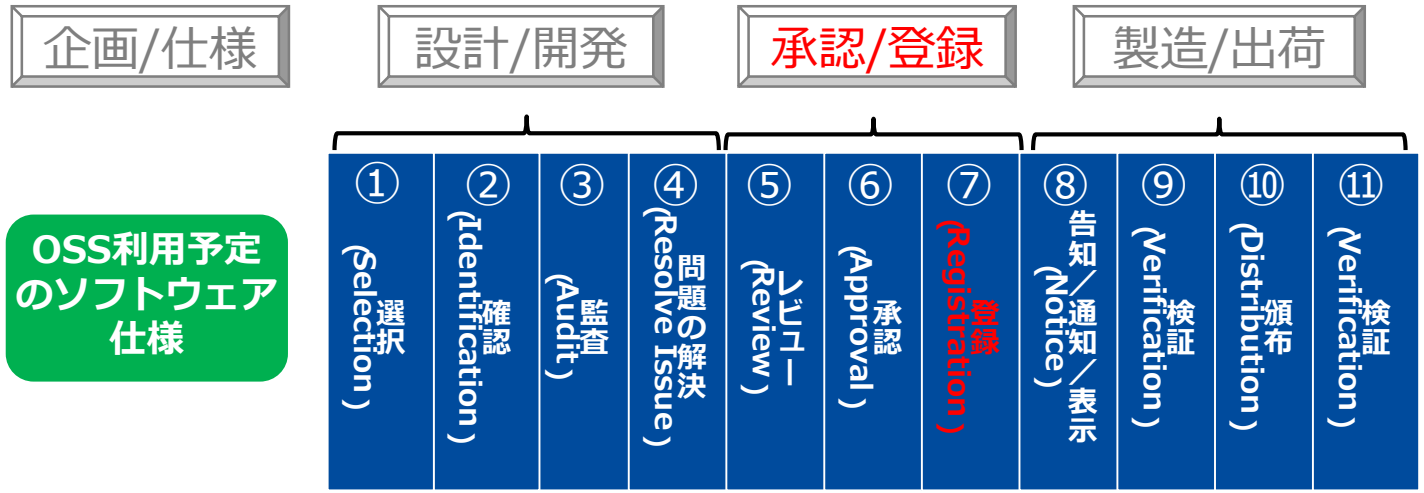


⑦ 登録

SW360(要検討)：

- OSS名、バージョン、社内担当者、使用するプロジェクト、プロジェクトのバージョン、など詳細を記録する

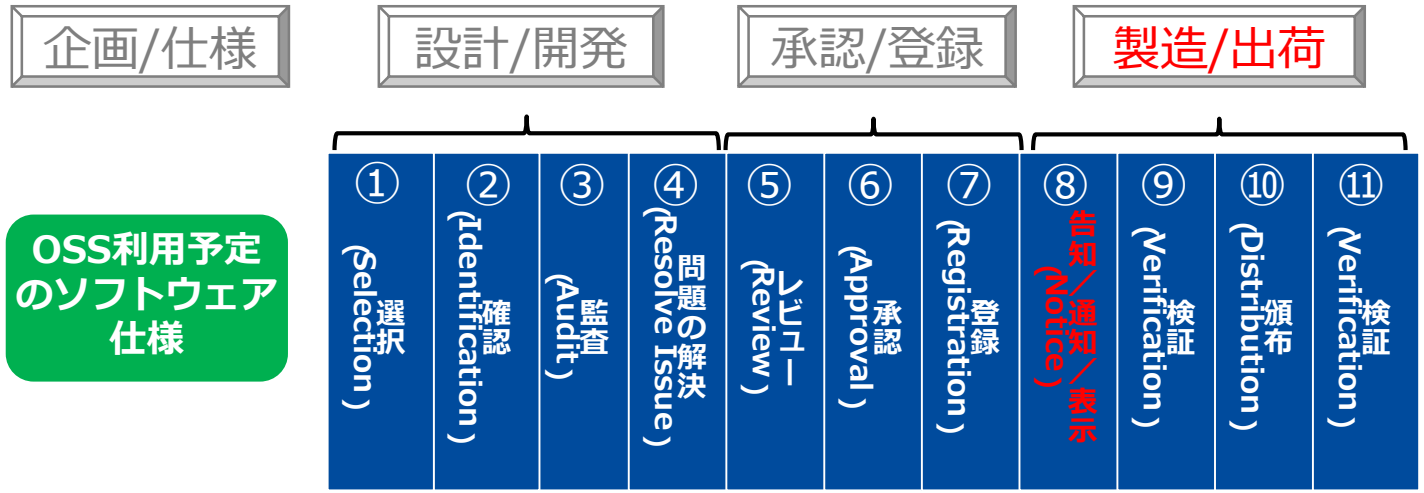
備考:現在 登録ルール/詳細検討中



⑧ 告知／通知／表示

SW360：

- 著作権リスト、ライセンスリストを成型する
- 製品添付文書のフォーマットを登録、文書出力する

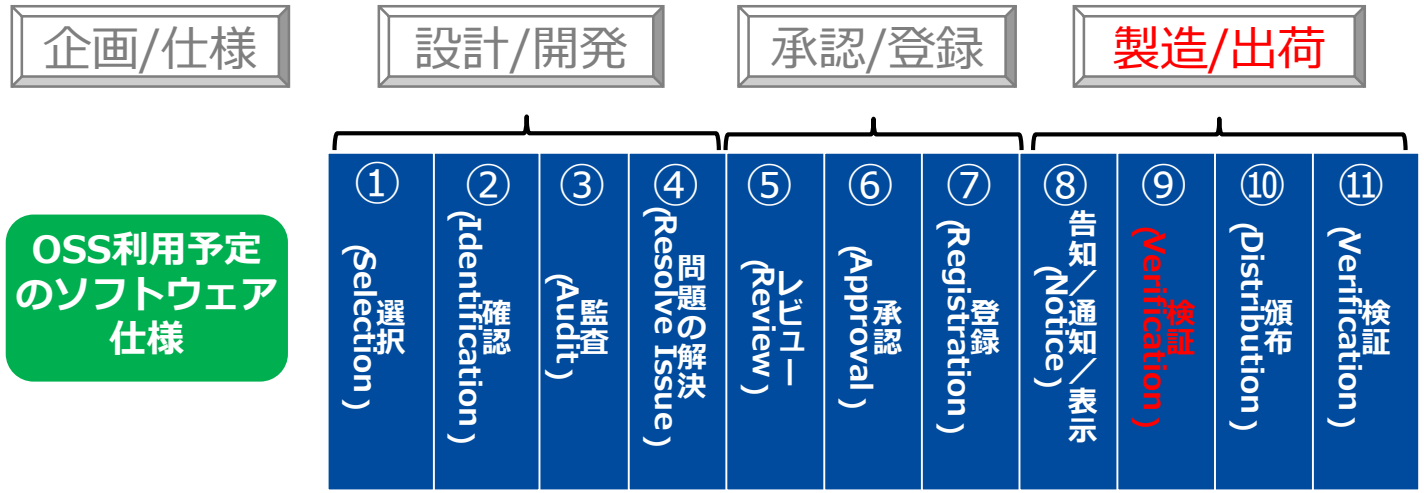


⑨ 出荷前検証

SW360(要検討)：

- ロ登録情報が正しいことを最終確認
- ロ告知文書等が登録されることを確認
  - OSSを含むコードの配布方法を決定/選択する
  - 配布用ソースコードと製品バイナリの一致を確認する
  - 告知文書がラインセンスを満たすことを確認する
  - 公開用ソースコードに余分な情報が無いようにする(コメント文など)

→ 実施状況・ワークフローを確認できるようにする



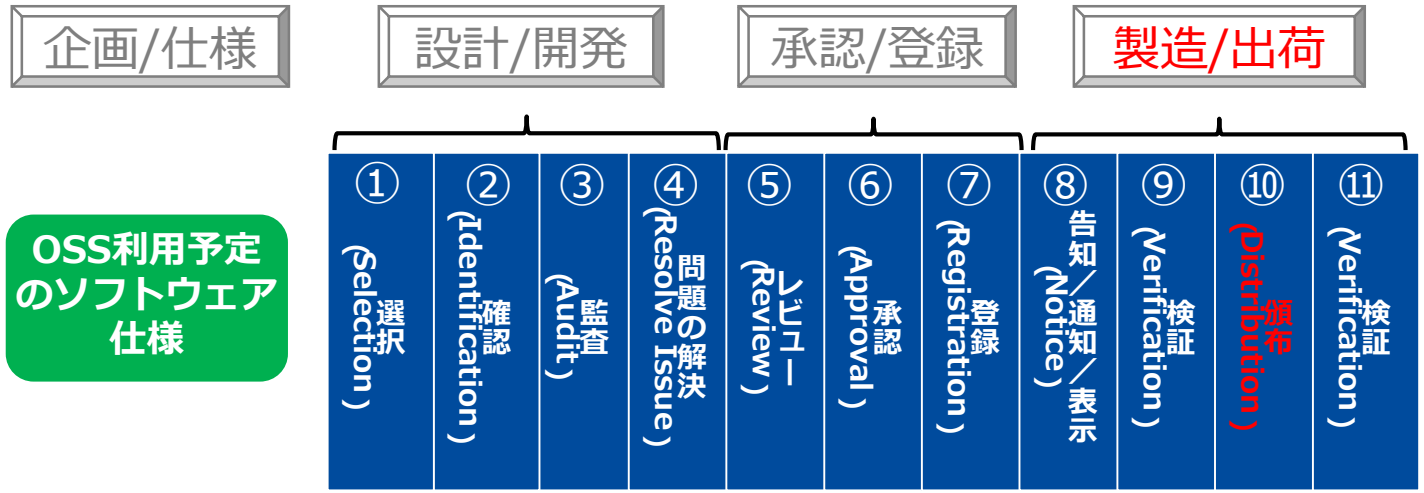
⑩ 頒布

SW360(要検討)：

- 頒布情報登録

  登録例：

  - 公開期間
  - 頒布用パッケージ
  - ソースコードを公開しているウェブページ



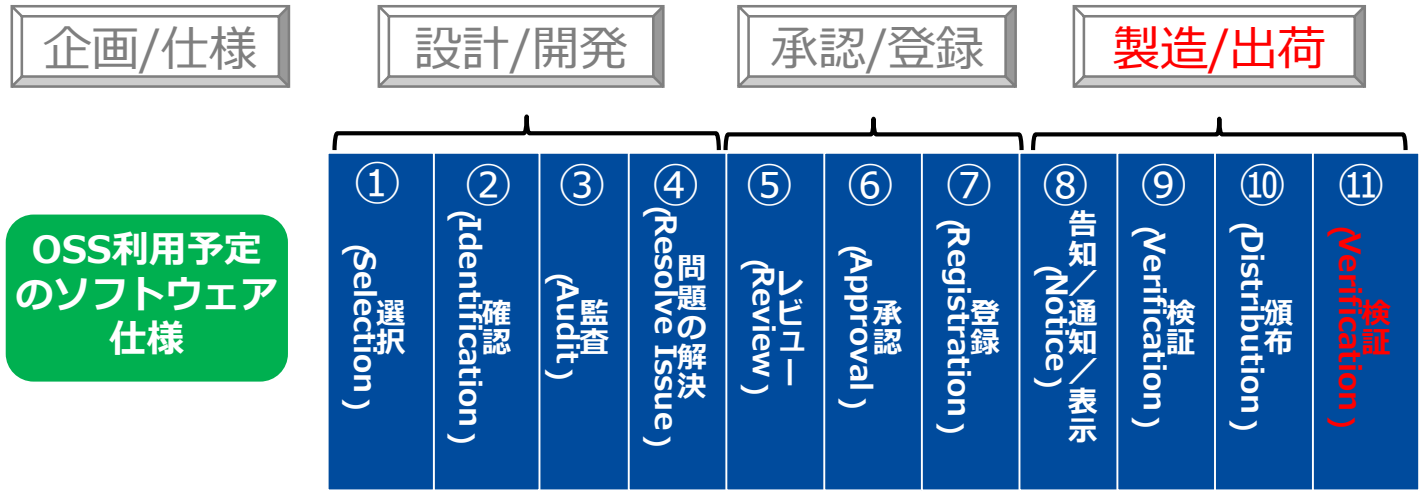
⑪ Verification

SW360 (要検討) ：

- Register the final verification results

  <u>やりたいこと</u>

  もしウェブ公開する場合は、公開しているサイトから正常にソースコードを入手し、解凍し、製品と同じものが入手でき、コンパイルができることなどを確認



03

おまけ

おまけ

Open Source Summit Japan　7月18日（木）
16:50-17:30

Using SW360 for OSS Complience Management Process - Kouki Hama , Toshiba

https://ossalsjp19.sched.com/event/OVtF/using-sw360-for-oss-complience-management-process-kouki-hama-toshiba

ご参加＆フィードバックお願いいたします！
Please　join！